Missouri Secretary of State Robin Carnahan
Records Services Division
presents:

Managing Electronic Records

Workshop 3 in the Missouri Electronic Records Education and Training Initiative

May 11, 2005
Presented by:
John Breeden, CRM

Provided under contract with:
*e*Visory

Outcomes

At the end of this session, you will understand:

- Why it is important to manage electronic records
- The legal requirements related to electronic records
- The types of electronic records produced by today's technology and some tips in managing them
- The technology that creates, stores, and allows retrieval/controls access of electronic records
- Steps to designing and implementing an electronic records system
- Design/implementation considerations, including requirements for and uses of metadata
- The roles played by records management and information technology in the management of electronic records

2

Benefits of Effective Electronic Records Management

- Meet statutory records retention obligations
- Protect organization against litigation and litigation costs
- Protect the integrity/authenticity of records
- Facilitate easy and timely access to records
- Control the creation and growth of records, reducing operating costs, storage costs, and migration costs
- Ensure proper access/security of records
- Protect vital records
- Preserve state and local government history and memory

3

Costs of Not Managing Electronic Records

- Fail to meet statutory records retention
- Litigation expenses and losses
- Can't find records
- Excessive operating costs, storage costs, and migration costs
- Confidential records made available inappropriately
- Records lost to disasters-Loss of history/memory

4

Electronic Records Legal Requirements

Federal Requirements

Code Citation Number	*Subject*	*Summary*
44 USC § 2902	Objectives of Records Management	Accurate and complete documentation of the policies and transactions of the Federal Government
44 USC § 3101	Documentation	Responsibility to make and preserve records containing adequate and proper documentation
36 CFR § 1220.34	Documentation	Adequate and complete documentation
36 CFR § Part 1222	Creation and Maintenance	Creation and Maintenance of Records; Adequate and Complete Documentation
36 CFR § 1222.34	Documentation	Ensure adequate and complete documentation
36 CFR § 1222.34	Records and Non-Records	Essential to distinguish between records and non-records
36 CFR §1222.34©	Working Files and Similar Materials	Drafts are records if they are circulated for comment AND contain substantive comments that add to a proper understanding of the formulation of the agency's decision
Federal Rules of Evidence	Valid Evidence	A data compilation in any form
Rule 902(11), Rule 902(12	Accepted evidence	Accepted evidence
Federal Information Processing Standards Publications FIP 196	Digital Signatures	Digital Signature Standard (DSS) -- 00 January 27
36 CFR 1234	Electronic Records	Electronic Records Management

6

US/State Requirements

- U.S. Privacy Act
- Electronic Signatures in Global & National Commerce Act
- Uniform Electronic Transactions Act (UETA-States)
- Laws vary by state but must follow or exceed Federal law
- Case law related to electronic records changing

7

Missouri Requirements

- Public and Business Records, RSMo Ch. 109
  - State and Local Records Law, RSMo 109.200 – 109.310
- Missouri Sunshine Law, RSMo Ch. 610

8

Signatures and the Law

- Signing writings serve the following general purposes:
- **Evidence:** A signature authenticates a writing by identifying the signer with the signed document. When the signer makes a mark in a distinctive manner, the writing becomes attributable to the signer.
- **Approval:** As defined by law, a signature expresses the signer's approval or authorization of the writing, or the signer's intention that it have legal effect.

9

What is a Digital Signature?

- A type of electronic signature that is generally considered the most reliable and secure. Digital signatures use public key infrastructure (PKI) to authenticate the sender and verify the information contained in the document. With the passage of the electronic signatures act, digital signatures are expected to become increasingly popular for exchanging information, conducting transactions and signing contracts over the Internet. www.cio.com/research/security/edit/glossary.html

10

How Digital Signature Technology Works

- **Digital signature creation** uses a hash result derived from the signed message and a given private key. For the hash result to be secure, there must be only a remote possibility that the same digital signature could be created by the combination of any other message or private key.
- **Digital signature verification** is the process of checking the digital signature by reference to the original message and a given public key, thereby determining whether the digital signature was created for that same message using the private key that corresponds to the referenced public key.

11

International Standards (ISOs)

- The ISO is a worldwide federation of national standards bodies
- The ISO pertaining to records, including electronic records is ISO 15489-1 and ISO 15489-2

12

ISO 15489-1 Scope

- ISO 15489 provides guidance on managing records of originating organizations, public or private, for internal or external clients
- Part of this ISO:
  - Applies to the management of records, in all formats or media, created or received by any public or private organization in the conduct of its activities, or any individual with a duty to create and maintain records

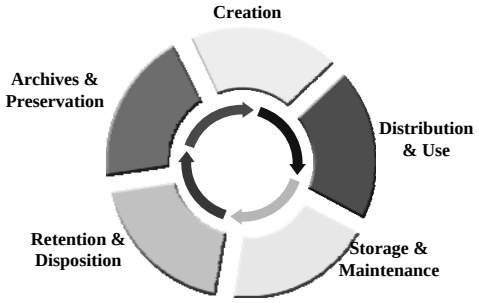
13

  - Provides guidance
    - on determining the responsibilities of organizations for records and records policies, procedures, systems, and processes
    - on records management in support of a quality process framework to comply with ISO 9001, Quality Management Systems and ISO 14001, Environmental Management
    - Provides guidance on the design and implementation of a records system, but
  - Does not include the management of archival records with archival institutions

14

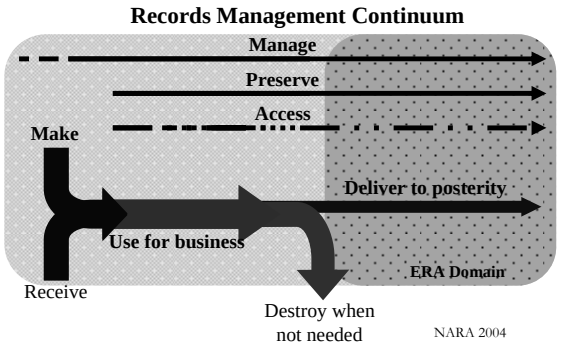
Electronic Records Basics

The Records/Information Management Lifecycle (ILM)



16

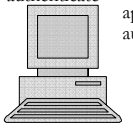
Archival Business Model: Context



17

Comparing and Contrasting Paper and Electronic Records Life Cycles

- Paper
  - Secure. Only available to those possessing paper.
  - Distribution can be difficult and multiple copies often result.
  - High storage costs.
  - Easy to identify and retrieve.
  - Relatively easy to authenticate in court.
- Electronic
  - Security must depend on technology applied.
  - Easy distribution from central storage locations.
  - Storage costs may be less or higher depending on technology.
  - Retrieval can be difficult unless additional coding, metadata, is applied. May be difficult to authenticate in court.



18

- Tracking can be done manually.
- Each paper or set of papers easy to identify as a record.
- Stable technology.
- Long storage life span.
- Easy disposal.

- Tracking requires technology system.
- May be difficult to determine what a record is.
- Changing technology.
- Technology affects life span.
- Disposal, due to distributive nature and need to employ technology can be difficult.

19

Electronic Record Types

Documents

- Desktop applications create electronic records that span multiple record series
  - Word processed documents
  - e-mail
  - spreadsheets
  - e-presentations
  - GIS/CAD systems
  - Images
- Retention must be based on what the records document, not their format; but too often retention and storage is controlled by the user and may be controlled from a desktop, network, document management system, etc.

Modified from slide by Gearhart

21

Identifying Documents by Extensions

- All electronic products of a computer application can be identified by the last three digits of the file name. This identification, called the extension, is usually preceded by a ".". Different applications use different extensions.

22

Common Document Extensions

Extension	Application and File Type
.AI	Adobe Illustrator file.
.AIF	Auto Interchange File Format (AIFF) Audio file.
.ANS	ANSI text file.
.ARJ	Compressed file can be used with Winzip / Pkzip.
.ASC	ASCII Text file
.ASP	Microsoft FrontPage Active Server Pages. To open these files use your internet browser.

23

B	
.BFC	Microsoft Windows 95 / Windows 98 Briefcase file.
.BK2	Corel Word Perfect for Windows Backup file.
.BK3	Corel Word Perfect for Windows Backup file.
.BK4	Corel Word Perfect for Windows Backup file.
.BK5	Corel Word Perfect for Windows Backup file.
.BK6	Corel Word Perfect for Windows Backup file.
.BK7	Corel Word Perfect for Windows Backup file.
.BK8	Corel Word Perfect for Windows Backup file.
.BK9	Corel Word Perfect for Windows Backup file.
.BMP	Graphical Bit Mapped File used in Windows Paintbrush.
.BPS	Microsoft Works Word Processor File.
.BPT	Corel Draw Bitmap master file
.BV6	Corel Word Perfect for Windows Backup file.

24

.CAL	Windows Calendar, Supercalculator4 file or Supercal spreadsheet.
.CDR	Corel Draw Vector file.
.CFL	Corel flowchart file
.CLP	Windows Clipboard / Quattro Pro clip art / Clipper 5 compiler script
D	
.DOC	Microsoft Word Windows/DOS / LotusWorks word processor Windows/DOS /PF S:First Choice Windows/DOS DOT MS Word Windows/DOS.
.DOS	Text file and DOS Specification Info
.DOT	Microsoft Word Template (Macro).
.DRW	Micrografx draw/graph files.
.DXB	Drawing interchange binary file
.DXF	Autocad drawing interchange format file

25

E – L	
.EQN	Word Perfect for Windows Equation file
.FDF	Adobe Acrobat Forms Document.
.FRK	Compressed zip file used with Apple Macintosh computers.
.GRF	Micrografx draw/graph files.
.IWA	IBM Writing Assistant Text file.
.JAS	Graphic
.JPG	Graphic commonly used on the Internet and capable of being opened by most modern image editors.
.JZZ	Jazz spreadsheet
.LWP	Lotus Wordpro 96/97 file.
M-O	
.MAC	Macintosh macpaint files.
.MBX	Microsoft Outlook Express mailbox file.
.MD	Compressed Archive file
.MPP	Microsoft Project file.
.MSP	Microsoft paint file format.
.MWP	Lotus Wordpro 97 smartmaster file
.MYD	Make your point presentation file.
.OLI	Olivetti text file

26

P	
.PAB	Personal Address Book, file used with Microsoft Outlook.
.PCX	Microsoft Paint & PC Paintbrush Windows/DOS.
.PDD	Adobe PhotoDeluxe Image.
.PDF	Adobe Acrobat Reader file.
.PLN	WordPerfect spreadsheet file
.PP4	Picture Publisher.
.PP5	Picture Publisher.
.PPS	Microsoft PowerPoint Slideshow.
.PPT	Microsoft PowerPoint presentation.
.PPX	Serif PagePlus publication.
.PPZ	Microsoft PowerPoint Packaged Presentation.
.PSD	Adobe Photoshop image file.
.PWP	Photoworks image file.
.PZA	MGI PhotoSuite album file.

27

R-V	
.RTF	Rich Text Format file.
.SDA	StarOffice drawing file / SoftCuisine data archive
.SDC	StarOffice spreadsheet
.SDD	StarOffice presentation
.SDL	SmartDraw library
.SDN	Small archive
.SDR	SmartDraw drawing
.SDS	StarOffice chart file / Raw MIDI sample dump standard file
.SDT	SmartDraw template
.SH3	Harvard (now Serif) presentation file
.SHK	Apple Macintosh Compressed Archive file
.SHW	Corel presentation / WordPerfect Slide Show / Show File
.SLK	Multiplan file. / Microsoft Excel symbolic link.
.SWF	Macromedia Flash file.
.TLP	Microsoft project timeline fie.
.UNX	Text file generally associated with UNIX.
.VC	VisiCalc Spreadsheet file.
.VSD	Visio drawing.

28

W-X	
.WB1	Quattro Pro Notebook
.WB2	Quattro Pro Spreadsheet
.WBF	Microsoft Windows Batch File
.WBK	Wordperfect document / workbook
.WG1	Lotus 1-2-3 worksheet
.WG2	Lotus 1-2-3 for OS/2 worksheet
.WK1	Lotus 1-2-3 all versions / LotusWorks spreadsheet.
.WK3	Lotus 1-2-3 for Windows /Lotus 1-2-3 Rel.3.
.WKS	Lotus 1-2-3 Rel lA,2.0,2.01, also file used with Microsoft Works.
.WPS	MS Works word processor Windows/DOS.
.WRI	Windows Write.
.WRK	Lotus 1-2 31.0,1.01,1.1/ Symphony 1,1.01.
.WRI	Symphony I.1,1.2,2 / Microsoft Write file.
.XIF	Wang image file / Xerox image file
.XLB	Microsoft Excel File.
.XLS	Microsoft Excel File.

29

Databases

- No single form, or group of fields in database is truly a record. The information must be used in relation to other data.
- In order for the data in the database to mean something, it must have both meaning and context. For instance, the name of a records series in a records management database has no real meaning until it is united with the other information including description, retention period, destruction method, etc.

30

Database Records

- A record in a database consists of:
  - Content (data)
  - Meaning
  - Structure (relationships and)
  - Context (an understanding of the reason for the data's existence
- Records may be made up of any or all of
  - Database tables
  - Individual database records (field information)
  - The entire database
    - State Archive Department, Minnesota Historical Society Mar 2004

31

Common Database Extensions

.$$A	OS/2 program file
.$$F	OS/2 database file
.$DB	DBASE IV temporary file
A	ADA program file or UNIX library
.AI	Adobe Illustrator file.
.DB	Paradox database file / Progress database file
.DB2	dBase II file
.DBC	Microsoft Visiual Foxpro database container
.DBF	dBase II,III,III+,IV / LotusWorks database.
.DBK	dBase databse backup / Orcad schematic capture backup file
.DBO	dBase IV compiled program file
.DBQ	Paradox memo
.DBT	dBase database text file
.DBX	Database file / DataBeam Image / MS Visual Foxpro Table
.DTF	Q&A database

32

.MDA	Microsoft Access Add-in / Microsoft Access 2 Workgroup.
.MDB	Microsoft Access Database / Microsoft Access Application.
.MDE	Microsoft Access Database File
.MDN	Microsoft Access Blank Database Template
.MDT	Microsoft Access Add-in Data
.MDW	Microsoft Access Workgroup Information
.MDX	dBase IV Multiple Index
.MDZ	Microsoft Access Wizard Template
.MVB	Database file / Microsoft multimedia viewer file
.MYD	Make your point presentation file.
	N
.NDX	Indexed file for most databases.
.NLB	Oracle 7 data file
	P
.PLI	Oracle 7 data description

33

	U
.UNI	MikMod (UniMod) format file / Forcast Pro data file
.UNK	Unknown file type, sometimes used when a file is received that cannot be identified
.UNX	Text file generally associated with UNIX.
.URL	File used with some browsers such as Internet Explorer linking you to different web pages. Internet Shortcut.
.VSS	Visio stencil.
.VST	Video Template / Truevision Vista graphic / Targa Bitmap/
.VSW	Visio workspace file.
.VXD	Windows system driver file allowing a driver direct access to the Windows Kernel, allowing for low level access to hardware.

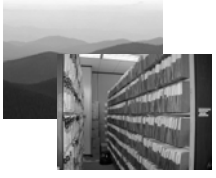
34

	W
.WDB	Microsoft Works database
.WFM	dBASE Form object
	Y
.Y01	Paradox index file
.Y02	Paradox index file
.Y03	Paradox index file
.Y04	Paradox index file
.Y05	Paradox index file
.Y06	Paradox index file
.Y07	Paradox index file
.Y08	Paradox index file
.Y09	Paradox index file

35

Images

- Images may be from art and drawing applications such as Adobe Photoshop, Corel Draw, or from architectural/engineering programs such as Auto Cad.



36

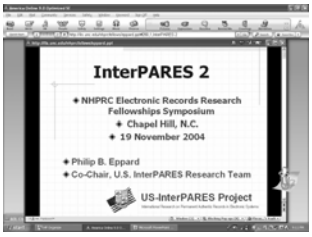
Imaging/Document Mgmt Systems

- Lines are blurring between the two but traditional imaging systems are used to retain paper records as images. Most of what we'll talk about today apply to these systems. A variety of AIIM standards and technical reports, including ARP-1 (Implementation Guidelines) are available.

37

Presentations

- Presentations may be created in several applications including:
  - PowerPoint
  - Presentware
  - Harvard Graphics



38

Spreadsheets

- Spreadsheets include but are not limited to:
  - Microsoft Excel
  - Lotus 1,2,3
  - Multiplan
  - StarOffice
  - VisiCalc

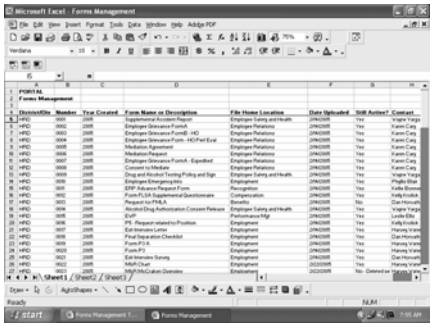
39

Flat File Databases

- There are two major types of databases
  - Flat file - A database that contains a single table and can be easily represented using plain text. This type of database contrasts with a relational database, which can contain any number of tables that are linked together. Often, to keep things simple when transferring data between organizations, people will request a flat file. Common flat file text formats include tab-delimited and CSV.

40

Flat File Illustration



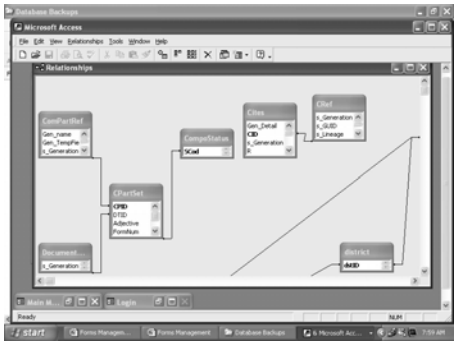
41

Relational Databases

- Relational databases store all their data inside tables. All operations on data are done on the tables themselves or produce other tables as the result.

42

Relational Database Illustration



43

Questions
Break

E-Mail and Instant Messaging

E-Mail vs. Instant Messaging

- e-Mail
  - used for inter-office communication
  - wide network of users
  - Can be used as a customer service function but there is a time delay between questions and answers
  - can reach you no matter what because the e-mail will be retained in the application until it is replied to or deleted
- Instant Messaging
  - used for inter-office communication
  - wide network of users
  - can be used as a customer service function allowing visitors to get instant personal assistance
  - can only reach you when you're online and want to be reached, an obvious advantage for anyone who wakes up to an in-box of 75 new messages, only two of which turn out to be worth reading

46

E-Mail and Instant Messaging as Corporate Records

- When an e-mail or instant message documents a business activity, it should be captured into a corporate recordkeeping system and managed as a record. There are a wide variety of software products, such as IMLogic that can capture and retain instant messages

47

Attachments

- Many times, important data is captured as an attachment to an e-mail. These attachments should be kept with the e-mail basic document.
- Instant messaging does not provide attachment features.

48

Protecting e-Mail and Instant Messaging

- Many people keep important e-mails in personal folders provided by the e-mail application, MS Outlook for example. This is an insecure place and does not offer the backup protection of a network server. E-mails are more secure when they are transferred to a network location, or archived on portable media.
- Because e-mails can be altered without detection, original e-mails imported into a document management system are more trustworthy for litigation purposes.
- Instant messaging is normally not transferable into another application.

49

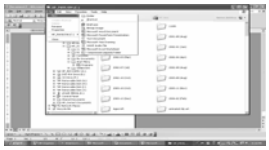
Transferring e-Mail

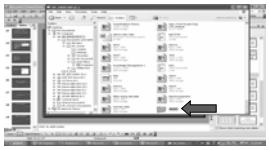
- Transferring e-mail in an application suite such as MS Office/Outlook is a relatively simple procedure. The metadata and any attachments are carried with the e-mail in rich text format.

50

How to Transfer E-Mail

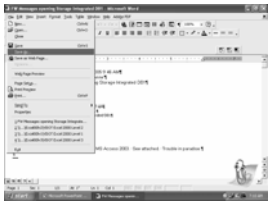
1. Create a folder using Explorer on the network or other storage medium in which to place the e-mail.
2. Name the folder with an easily identifiable tag, i.e. records series, project name, personnel file name, etc.
3. Open the e-mail application, we are using Outlook since it is widely used.
4. Select the e-mail you want to transfer.
5. Open the e-mail.

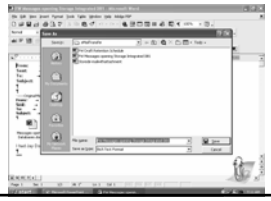




51

6. Select file, save as.
7. Select the folder you have created.
8. Name the e-mail file. You can use the subject line or a description of its purpose or association with a master file.
9. Click on save.

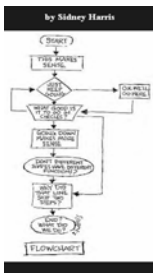




Your e-mail is now copied into the folder you selected. Any attachment will open if it is double clicked.

53

Electronic Records Technology Functionality



Access Control

- Access control software must be able to permit or deny individual users access to read individual records and files. More sophisticated access control (e.g. controlling access to collections of records, or restricting certain groups of users) may be required by a public office. Public offices should carefully evaluate the administrative costs of managing access control policies to determine the most cost-effective way of achieving the necessary security.

55

Information systems vs Recordkeeping systems

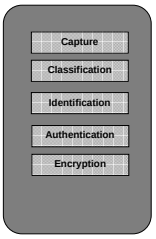
Information systems	*Recordkeeping systems*
Timely	Time bound
Manipulable	Inviolable
Non-redundant	Redundant

Recordkeeping Forum

56

Overview

- Electronic recordkeeping systems uniquely capture, classify, and identify records in order to ensure that their content, structure, and context of creation is fixed in time and space.



Recordkeeping Forum New Zealand

57

Capture

- Records:
  - diverse formats
  - may be compound, i.e. images, text, spreadsheets, etc. – can be created and transmitted in a variety of ways – on a single computer drive, through a network to a server, on a Personal Digital Assistant (PDA), by scanning, etc.
- The content, structure and context of records must be captured to ensure that records are reliable and authentic evidence

58

Classifying

- Identified on a records retention schedule which groups them together based on their business function

59

Identifying

- Given a unique identifier such as a schedule number and records series which readily identifies the business group to which they belong and their purpose

60

Maintaining

- Must be retained in their original context until they may be destroyed or archived so their legal context is preserved

61

Protecting

- Access must be controlled so that only authorized individuals see appropriate records
  - Sunshine law exemptions
  - Privacy Acts
  - Critical Infrastructure Information
- Must have audit trails
- Must have location tracking

62

Retention and disposal

- Disposal authorities must legally authorize disposal of records from recordkeeping systems, whether by destruction or by transfer to another agency.
- Destruction must be documented.

63

Transfer/Migration

- The electronic system must have the capability to transfer records to other systems in case of reorganization or the requirement to upgrade based on new technologies.

64

Dissemination

- The electronic system must provide search, retrieval, and delivery of records to authorized users.

65

Administering

- Electronic records systems must provide access to systems administrators so that they may perform maintenance and support. Administrators include traditional IT but also records managers and end-users who manage components of the systems.

66

Administration

- In exceptional circumstances, records may be altered or deleted by system administrators.
- Additionally,
  - System administrators will sometimes be required to create copies of records without sensitive information (redacted copies).
  - System administrators also need to be able to manage system parameters, back up and restore data, and generate system reports.

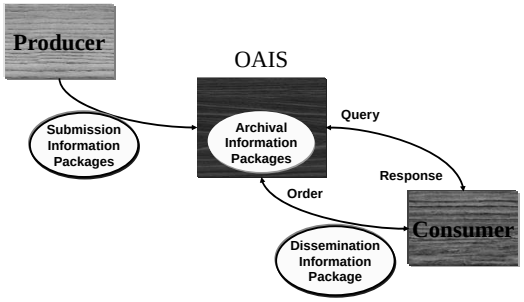
67

One Example System: Capabilities of NARA's Electronic Records Archives (ERA)

68

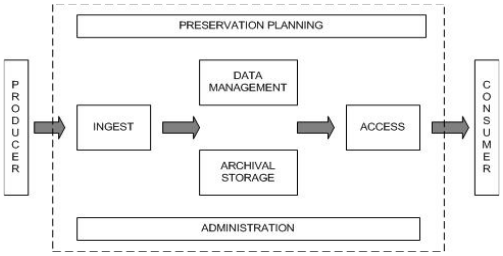
NARA's ERA System

An Open Archival Information System



69

NARA Reference Model for an Open Archival Information System



70

What must the system do?

- Support the collection, integration, and sharing of metadata about records
- Support the workflow associated with business processes
- Interface with other systems
- Maintain a complete audit trail
- Accommodate growth and technological changes
- Protect the system and the records with state-of-the-art security

NARA and ISO 15489-1:2001 (E)

71

- Process electronic records regardless of format
- Manage permanent and temporary electronic records
- Maintain relationships among records
- Store records reliably
- Make electronic records independent of specific hardware and software
- Manage records according to their sensitivity

NARA and ISO 15489-1:2001 (E)

72

- Implement record schedule retention and disposition requirements
- Allow appraisal of electronic records
- Manage disposition of electronic records
- Allow review and redaction of sensitive information by authorized personnel

NARA and ISO 15489-1:2001 (E)

73

For Records Users, the System Must

- Provide search functions based on records descriptions
- Allow authorized users to do searches without assistance
- Accurately reproduce and output electronic records
- Provide certified copies of electronic records
- Manage requests for review of restricted materials
- Enable users to request and receive assistance from records management staff

NARA and ISO 15489-1:2001 (E) 74

Updating Technologies

- Hardware
  - Systems must be able to migrate data to new hardware, i.e. servers, optical media, etc.
  - Systems must be able to accept input from new peripheral devices.
  - Systems must be able to communicate over new transmission technologies.
- Software
  - The system must be able to accept records developed in new applications, upgrades to old applications.

75

Regulatory Issues

- The system must be programmable so that new records retention requirements such as digital signatures and other requirements placed on records management by Federal and State laws can be complied with.

76

Retrieval Issues

- The system must be able to accommodate retrieval by new hardware and software programs as they are developed such as the integration of cell telephone and computer technology, advanced personal assistance devices, wireless devices, etc. while maintaining records security.

77

Backup & Restoration vs Disaster Recovery

- Backup - To copy files to a second medium (a disk or tape) as a precaution in case the first medium fails. One of the cardinal rules in using computers is to back up your files regularly. To be especially safe, make more than one backup and keep one in a different location from the others. You can back up files using operating system commands, or you can buy a special-purpose backup utility.
- Restoration – Orderly restoration of data from backup media following system failure.

78

Backup & Restoration vs Disaster Recovery

- Disaster Recovery - The salvaging of data stored on damaged media, such as magnetic disks and tapes. There are a number of software products that can help recover data damaged by a disk crash or virus. In addition, there are companies that specialize in data recovery. Of course, not all data is recoverable, but data recovery specialists can often restore a surprisingly high percentage of the data on damaged media.

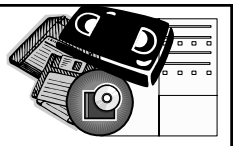
79

Disaster Recovery

- The system must provide a means of recovering from disasters such as:
  - natural events such as earthquakes, tornados, fire, floods
  - structural or building failure such as malfunctioning sprinklers, heating or air conditioning systems, leaks in roofs, poor wiring
- technological disasters such as viruses and computer equipment failures
- criminal behavior such as theft, arson, espionage, vandalism, riots, terrorism and war, and
- accidental loss through human error

80

Backup and Restoration



- The system must allow complete and frequent backups of all data so that it may be stored off site. Typical backup media are:
  - Floppy diskettes, Zip® disks, Jaz® disks, and the like
  - Writable CDs, writable DVDs, and other types of optical media
  - Tape
  - Another hard drive or another computer

81

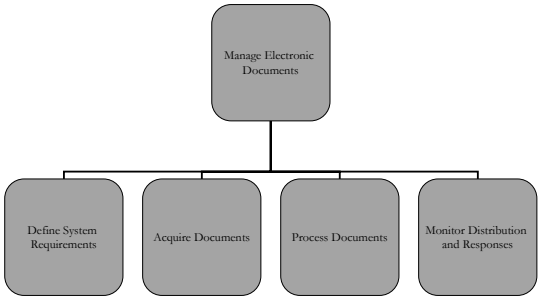
Questions Lunch

82

Designing and Implementing Electronic Records Systems

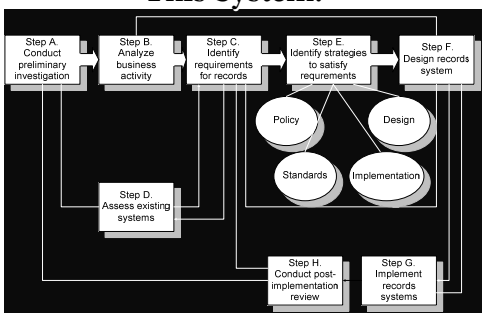
(Adapted from ISO 15489)

What Should a System Look Like?



84

How Do I Design and Implement This System?



85

Step A. Preliminary Investigation

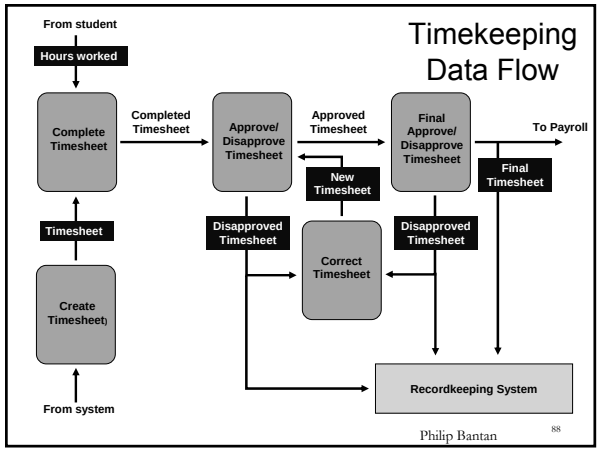
- Understanding of the following contexts:
  - Administrative
  - Legal
  - Business
  - Social

86

Step B. Analysis of Business Activity

- Develop a conceptual model of what the organization does and how it does it to demonstrate how records relate to business and business processes.

87



Philip Bantan

88

Step C. Identification of Requirement for Records

- Identify an organization's requirements to create, receive, and keep records.
- Document the requirements in a structured and easily maintainable form.
  - A list of all sources containing records requirements
  - A list of regulatory, business, general community requirements to keep records
  - Risk assessment report endorsed by management, and
  - A formal requirements document for management and staff

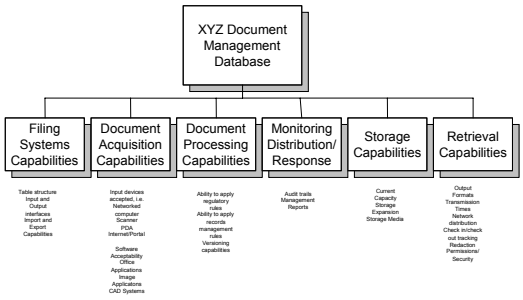
89

Step D. Assessment of Existing Systems

- Measure existing systems' ability to capture and maintain records.
  - Inventory of existing business systems
  - Report outlining the extent they actually meet the agreed requirements for records

90

Sample Assessment Chart



91

Step E. Identify Strategies

- Policy – Sample from Government of New South Wales: Take into account that:
  - Agencies' electronic records are official records
  - Electronic recordkeeping should comply with recognized best practice
  - Electronic recordkeeping should be built into business processes and tools
  - Business conducted by electronic means should be adequately documented to meet identified recordkeeping requirements
  - Electronic records should be maintained in electronic form
  - Electronic records should be maintained in reliable recordkeeping systems
  - Electronic records should be managed effectively as part of a comprehensive records management program
  - Maintaining and providing access to electronic records over time is a shared responsibility

92

Step F. Design Records System

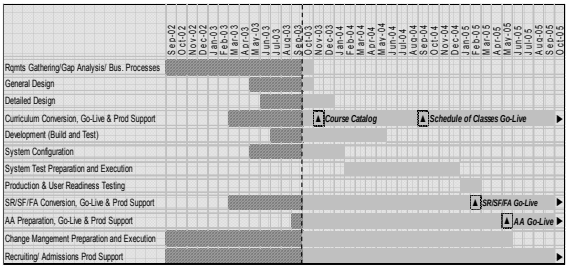
- Records Management, Information Technology and end users together
  - Design project plans, tasks, responsibilities, timelines
  - Outcome reports of design reviews
  - Changes to requirements
  - Descriptions
  - Systems Specifications
  - Diagrams of systems architecture, components
  - System business rules

93

- Models of processes, data flows and data entities
- Detailed specifications to build or acquire technological components – hardware, software, etc.
- File plans
- Plans showing how the design will integrate with existing systems and processes
- Initial training and testing plans
- Systems implementation plan

94

Sample Project Plan Timeline



95

Sample Design Document Contents - DoD 5015.2-STD

- Taken from "Design Criteria Standard for Electronic Records Management Software Applications"
- To view/print entire report, click on following URL: http://www.dtic.mil/whs/directives/corres/pdf/50152std_061902/p50152s.pdf
- CHAPTER 2- DETAILED REQUIREMENTS
  - C2.2.1. IMPLEMENTING FILE PLANS
  - C2.2.2 SCHEDULING RECORDS
  - C2.2.3 DECLARING & FILING RECORDS
  - C2.2.4 FILING ELECTRONIC MAIL MESSAGES
  - C2.2.5 STORING RECORDS
  - C2.2.6 RETENTION AND VITAL RECORDS MANAGEMENT
    1. Screening Records
    2. Closing/cutting off records folders
    3. Litigation Freeze/Unfreeze
    4. Transferring records
    5. Destroying records

96

DoD 5015.2 Tables

C2.T1. File Plan Components
C2.T2. Record Folder Components
C2.T3. Record Metadata Components
C2.T4. Transmission and Receipt Data
C2.T5. Authorized Individual Requirements
C4.T1. Classified Record Components
C4.T2. Authorized Individual Requirements

97

Sample System Business Rules

- **Business Rule**: An executable command within the system that implements a policy or a domain requirement, either uniformly or under specified conditions.
  - *Business Rule*: Any transaction in ERA to bring records into the system or remove them from it must conform to an authorized schedule item

NARA

98

Sample System Specifications

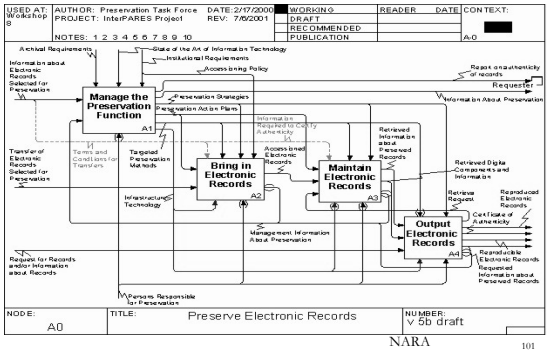
- **Functions:**
  - Storage pools
  - Policy-based file space provisioning
  - Storage quota management
  - Locking
  - Caching
  - Automated volume drain for volume migration
  - Data-copy migration tool

99

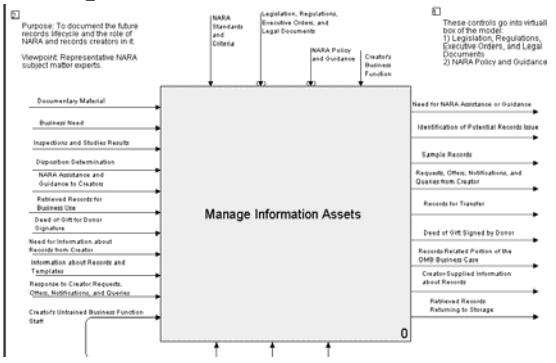
- **Interoperability:**
  - Hosts: IBM AIX, AIX HACMP, Microsoft Windows 2000 Server, Windows 2000 Advanced Server
  - Storage: IBM Enterprise Storage Server, SAN Volume Controller, SAN Integration Server
- **Management:**
  - Open standards/Storage Management Initiative Specification (SMIS) support, GUI, command line interface (CLI)
  - Call home and remote support
  - SAN management-Tivoli SAN Manager Bonus Pack

100

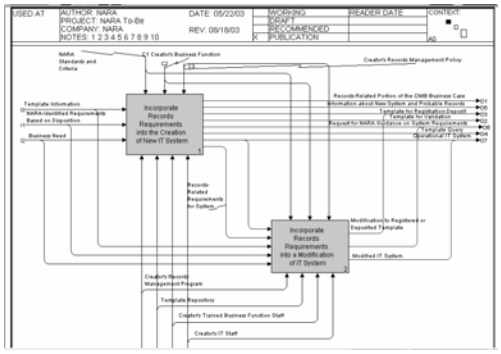
Sample System Architecture Design



Sample Process Model – NARA ERA



Sample Integration of ERA - NARA



103

Step G. Implementation

- Detailed project plan
- Documented policies, procedures, and standards
- Training materials
- Conversion process and migration procedures
- Quality system accreditation documentation
- Performance reports (System testing, user acceptance testing, etc.
- Management reports

104

Step H. Post Implementation

- Post-implementation review
- Periodic checks on system
- Documented system performance and development process
- Management report including findings, best practices, and recommendations
- Migration/Upgrades

105

Design/Implementation Considerations

106

Sample Environmental Controls

- Network
  - Establish a central authentication service.
  - Investigate and implement a central authentication service using public key and/or shared-secret key security standards

107

- Physical
  - All inbound dial-up lines (e.g. modems) and real-time external connections (e.g., Internet) connected to the networks carrying data must pass through an additional access control point (e.g., firewall) before authorized users reach the log-in banner.

    All in-bound dial-up lines to computer systems are protected with extended user authentication systems as technically and reasonably possible.

  - Computer rooms are secured and maintained under specific temperature and humidity controls.

108

Use

- Data security consists of procedures that prevent unauthorized access to your computer resources. Appropriate security procedures should not significantly hinder a person from performing their work. Security procedures should, however, protect data from unintentional acts, as well as intentional ones. Examples include:
- Select appropriate password safeguards
- A hard to guess password
- Periodic password changes
- Seven or more alphanumeric characters per password
- Passwords kept confidential

109

- Screen-saver passwords
- Assign each user a unique user ID (no shared user IDs)
- Limit user access to system software
- Control access to specific applications and data files
- Limit access to what is required to perform a person's job function and to allow for appropriate segregation of duties
- Review security logs
- Limit concurrent logins
- Activate intruder detection and prevention mechanisms
- Implement adequate virus protection procedures

110

Storage

- Desktop Computers
- Servers
- RAID Array (optical disk)
- Portable Media

111

Media Capacities

Medium	Capacity (Uncompressed)
Magnetic Media	
Removable hard disk	10 GB +
Removable disk	1.44 – 120 MB
Cartridge	10-30 GB
Magnetic Tape	20-180 MB
Digital Audio Tape (DAT)	24+ GB
Videotape	Up to 8 hours of video
Optical Media	
CD	650-800 MB
WORM (CD-R)	650-800 MB
Electro optical, i.e. laser, photometry, etc. (EO)	128 MB-1 GB
DVD	4.7 – 17 GB
Redundant Array of Independent Disks (RAID)	254 GB+ (depends on number of disks deployed)

112

Active Access

- Interoperability and connectivity to remote offices
- Employees access, view and maintain records
- Queries, reports, analysis
- Application interoperability, real-time connectivity and transaction processing

113

Metadata

- Each record, record series and folder maintains a set of *metadata fields*. Every metadata field has a human readable name or designator, and corresponding data that can be stored in the field. Some fields are *mandatory* and every object must be assigned valid data into these fields when filing, while other fields can be filled in optionally. The RMA should automatically fill and maintain fields as is reasonable and appropriate, although it must also provide for specifically user-created fields. There must be facilities to search for objects by field contents. The RMA must have a way to constrain the type of data that can be entered for a field. The RMA must limit the general editing of all metadata to the time of filing, except for authorized users who will have the ability to edit and correct filing errors. It should be noted that if a user does not have rights to edit a mandatory template field that is not auto-populated, they will not be able to file records using that template.

114

Linking

- The RMA must allow the users to define and establish relationships between documents, in the form of *document links*. Each link type has a unique human readable name, and each link contains the identifier of the source and linked to documents. There must be a way to view which documents are linked to, linked from, and by which link type for each document. There may also be a need to define (or allow for the defining) of events based on these links. Some examples of document links are superceded/successor records, multiple renditions, email/attachments, supporting documents and incremented versioning. As a form of metadata, document links can be established by all users at the time of filing and created/modified/removed post-filing by authorized users only.

115

Versioning

- The RMA must allow the users to establish record versioning, which is a special case of document relationships. Versioning is used to indicate an auto-incremented sequence of revisions to a particular record. Versions must all be retrievable as if they were independent documents and contain their own metadata, although the metadata for new versions can be based on that of a prior version. Versions can also be spread among multiple record series and have independent dispositions. The RMA must clearly indicate if a record is involved in versioning and if it is the most recent version.

116

Security Markings

- The RMA must allow the RM to define *Security Markings,* and to allow users to assign markings to records upon filing. These markings serve as a security based metadata field and are intended to define and restrict access as well as aiding in classification and retrieval. The RMA may also allow the RM to define *informational markings* at the time of filing. These markings are non-security metadata, and are intended solely as an aid to classification and retrieval. The presence of this second form of markings is not mandated by the RMA requirements. Regardless of being security-based, only authorized users can modify/remove Supplemental Markings post-filing.

117

Identification Metadata

Title	Purpose	Metadata Source
Category Type	Identifies the type of record using document extensions	Application
Identifier	Uniquely identifies a record	Form Number, Document Version
Title	Name of the record/document	Author and Application Properties
Creation Date	Date record was created	Application

118

Storage Metadata

Title	Purpose	Source
Store Location	The archive destination for the record.	Application. When you execute Save As you can determine the final destination.
Current Location	The original storage site for the file.	Application. Save or Save As command until the file is ready to archive

119

Relational Metadata

Title	Purpose	Source
Function	Describe business function	Application or text data dictionary
Related entity identifier	Identifies related record	Application, Records Schedule
Relationship Type	Version Control	Application, File naming convention
Creator	Identifies originator	Application. Automatic
Responsible Organization	Identifies organization of creator	Application

120

Access Metadata

Title	Purpose	Source
Access rights	Identifies staff allowed to access files	Application, Permissions established on servers, etc.
Access restrictions	Identifies Sunshine exemptions, security restrictions, etc.	Application passwording, server permissions, etc.

121

Records Management Metadata

Title	Purpose	Source
Registration date	Authenticates date record captured into system	Application
Preservation-storage	Information about the media and format in which electronic records are stored	Index, database, application history file

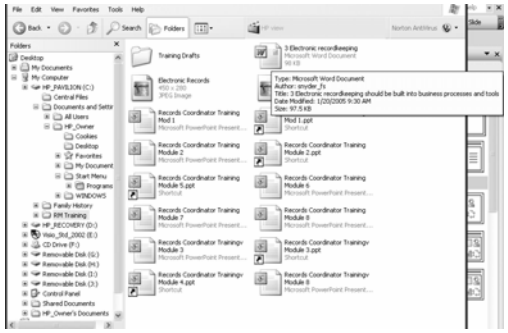
122

Records Management Metadata

Title	Purpose	Source
Preservation-Migration	Tracks migration activities	Project plans
Disposal Authorization	Provides legal authority to store, dispose	Records Retention Schedule, Metadata base
Event Management and authorizing official	Shows the management of the record over time – transfer to storage, destruction or archiving, etc.	Paper documents, database

123

Sample Identification Metadata



124

Adding Identification Metadata

The following example is based on Microsoft applications.

1. Locate the File Menu and left click on Properties.

125

2. Open the Properties Box.
3. Click on the Summary Tab.
4. Complete the information under this tab.

126

Additional Metadata

5. On the **File** menu, click **Properties**, and then click the **Custom** tab.
6. In the **Name** box, type a name for the custom property, or select a name from the list.
7. In the **Type** box, click the type of property you want.
8. In the **Value** box, type a value for the property. The value you enter must match the selection in the **Type** box. For example, if you click **Number** in the **Type** box, you must type a number in the **Value** box. Values that don't match the property type are stored as text.
9. Click **Add**.

127

E-Mail Metadata

- **From:**TheRose2272@aol.com
- **Date:** Tue, 29 Mar 2005 17:54:03 EST
- **Subject:** Hello there!
- **To:** vacatlady2000@yahoo.com

128

Preserving e-Mail

- e-Mail stored in Personal Folders is usually disconnected from applicable attachments.
- Personal folders can be lost even when they are housed on network drives and the cost of recovery can be very high.
- To really handle your e-mails and add additional metadata, transfer your e-mails and their attachments to a network drive or portable storage medium.

129

Inactive Storage

- Sufficient capacity
- Ability to electronically delete records
  - Must be able to completely erase records relating to privacy, security, etc.
- Reports on inactive storage activity
- Ability to maintain all formats of records with inactive status

130

Retention Schedules

- Retention schedules need to be updated to accommodate electronic records
- The inventory should include but are not limited to:
  - Type of electronic record
  - Software used
  - Name of system
  - Hardware used
  - Table structure
  - Type of transactions

131

Inventory

- **Electronic System Inventory**
  - Identifies the information contained in, the purpose of, and the technical attributes of the system

132

Inventory

- **Steps to Conduct an Inventory:**
  - Determine targeted offices; team members; timetable; etc.
  - Interview creators, users, and administrators of the system.
  - View the system on-line
  - Gather background information on system's purpose.
  - Document information gathered from each inventory.

133

Inventory

- **For Electronic Information Systems, you need to collect Information on:**
- Inputs
- Master Files
- Outputs
- Documentation
- Indices, queries, and sorts
- Backups

134

Inventory

Crucial questions

1. What is the name of the system?
2. What is the purpose of the system and which agency programs does it support?
3. What is the content of the system and what dates does it cover?
4. Does this system link to or support any other system?
5. Which records are temporary and what the retention period should be?
6. Which records are permanent and when to transfer to archives?

135

Analysis and Appraisal

- **Agency recommends:**
- Which records are temporary
  - And what the retention period should be
- Which records are permanent
  - And when to transfer to Archives

136

Schedule

- **For electronic information systems, you may consider:**
  - Scheduling the entire system as one item
  - Scheduling each of the system components as a separate item

137

Scheduling Databases & Other Electronic Records

- **For scheduling by system components:**
  - Description and disposition of
    - input records
    - master data files
    - outputs
    - documentation
    - related indexes, queries, and sorts

138

Schedule

- **Sample temporary disposition for inputs to electronic information system:**
  - Temporary. Delete or destroy after input and verification of data into master file or when no longer needed to support the reconstruction of master file, whichever is later.

139

Schedule

Sample dispositions for permanent master data file:

- Permanent. Transfer annual snapshot to archives.
- Permanent. Transfer to archives five years after close of operation.

140

System Tools

- Search capabilities
- Queries, reports, etc.
- Versioning
- Automatic application of records management disposition schedules
- Backup software
- Disaster recovery routines

141

Metadata Mining

- Definition
  - extraction of implicit, previously unknown, and potentially useful information from metadata.
- Methods
  - classification, clustering, summarization, mining association rules, ontology extraction, information integration, keyword extraction, automatic title generation.

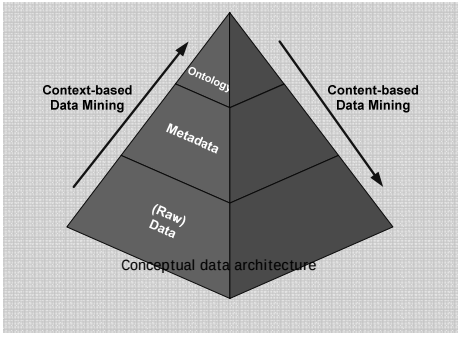
142

Metadata Mining

- Why metadata mining?
  - No access to the data itself, lack of raw data
  - The data is not convenient for mining (heterogeneous formats and non-text format)
  - Diversity of metadata standards, and need to merge different metadata repositories
  - Ontology extraction is much easier in metadata level

143

Metadata Mining



144

Where Do I Mine?

- e-mail (sent, received, or drafted) and corresponding dates, times, recipients, and
- file attachments
- word-processing files
- tables, charts, graphs, and database files
- electronic calendars
- proprietary software files
- Internet browsing applications (bookmarks, cookies, history log)

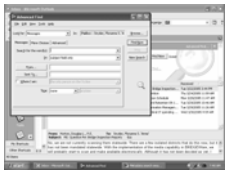
145

Mining for e-Mails

1. Open Tools, Find
2. Enter search criteria

146

- The list of e-mails containing search key words will appear
- When key words do not yield results, use advanced find



147

Desktop Issues

- Security
- Legal provenance
- Lack of backup
- Lack of control over destruction
- Copies existing on portable media
- Lack of security
- Storage
- Backup and disaster recovery

148

Final Disposition

- System must notify users of potential disposition
- Electronic files require special software to totally erase individual records without destroying drives
- Disposition forms must be entered in system to document legal destruction

149

Final Disposition

- System must be designed to allow destruction of electronic records at the end of their retention periods-don't combine records with different retentions on fixed media.
  - Storage may be inexpensive but still costs money and electronic records must be migrated unless they are legally destroyed
  - Records not destroyed are subject to legal discovery

150

Roles and Responsibilities

Records Management

- Develop and maintain the infrastructure of the system
  - Records Inventory
  - Records Schedules
  - Fileplans
  - Resolving records related issues
  - Determine operational configuration and behavior of the system
  - Ensure users are trained or train end users
  - Provide user assistance

152

Records Administrator

- Manage day to day operation of electronic management
  - Administration of filing structure
  - End user assistance to properly classify and organize records
  - Carry out routine disposal, transfer, and export activities

153

System Administrator

- Be the single point of access at which actions like folder and records deletion takes place
- Maintain the system activity
- Back up the system
- Take "system snapshots" on scheduled basis
- May create queries, reports, provide audit trail information
- Provide user assistance in technology related problems

154

Reviewer (Optional)

- May be the client, policy, records management
  - Assess the value and disposition of existing records in relation to disposition

155

End User

- Create records
- Categorize or verify categorization of records according to retention schedule
- Use records
- Retrieve records
- May create records folders in system if this is not assigned to records staff

156

Information Technology

- Obtain information about system design from records management staff
- Design system, models, etc.
- Create system documentation
- Assist in writing RFPs, RFQs, IFBs, etc.
- May be the actual purchaser of system
- Write test plans
- Implement system
- Evaluate system

157

Some Points to Remember

- Electronic records are complex with technology changing daily but they are still records that must be managed
- Because of changes in technology, there are no easy answers but there are standards, best practices, and vendors that can help you

158

Some Points to Remember

- Records Management MUST be a part of the initial design to ensure access, security, vital records protection and retention requirements are addressed
- End-users/Records Management/IT all have important roles to play in ensuring the successful implementation of electronic record keeping systems

159

For Help

- Missouri Secretary of State Records Services Division
  http://www.sos.mo.gov/records/
- Records Management 573-751-3319
- Local Records 573-751-9047

160

For More Help

- Association for Information & Image Management http://www.aiim.org/index.asp
- Association of Records Managers and Administrators http://www.arma.org/
- National Archives and Records Administration http://www.archives.gov/

161

Questions?

John Breeden, CRM
JLJBreeden@aol.com
804-338-6384